United Nations

A/59/116/Add.1*

General Assembly

Distr.: General
28 December 2004
English
Original: English/Spanish

Fifty-ninth session
Agenda item 60
Developments in the field of information and telecommunications in the context of international security

Developments in the field of information and telecommunications in the context of international security

Report of the Secretary-General**

Addendum

Contents

Page

Replies received from Member States

Mexico 2

United States of America 3

Venezuela 6

* Reissued for technical reasons.

** The information contained herein was received after the submission of the main report.

04-47511* (E) 100105

Replies received from Member States

Mexico

[Original: Spanish]
[18 August 2004]

1. In our times, marked by an astonishing development of information systems and telecommunications, the international community has grown aware of the fact that, going hand in hand with that advancement, the interconnection of users of those systems has come to be of such magnitude and such varied nature that the territorial and judicial frontiers of States have been overstepped.

2. This high degree of interrelatedness has brought with it a directly proportional level of vulnerability in the sphere of national and international security, thus confirming that telecommunications systems and information are strategic areas that have a great impact on the conditions of international peace and security.

3. For these reasons, Mexico considers that the means to be adopted to limit the threats arising in this field, in addition to being consistent with the need to preserve the free circulation of information and promote the development of those tools for peaceful purposes, must bring tangible benefits in the areas of disarmament and non-proliferation, draw nations closer together and facilitate greater cooperation in this domain.

4. The field of information and telecommunications, Mexico believes, must be examined from a dynamic and forward-looking standpoint, owing to the fact that the rapid rate of scientific and technological development has inevitably created a gap between the standards to be complied with and the actual capacities of such systems, resulting in an immediate increase in potential and real threats in the area of information security.

5. In view of the current relevance of the topic and the importance of studying concepts that will enable us to refer to this phenomenon with greater precision so as to be able to deal with it effectively, Mexico applauds the work commenced in February of this year towards establishing a group of governmental experts to collaborate with the Secretary-General of the United Nations on the elaboration of a study pertaining to the examination of "existing and potential threats in the sphere of information security and possible cooperative measures to address them", as well as "relevant international concepts aimed at strengthening the security of global information and telecommunications systems", as set out in paragraphs 4 and 2, respectively, of resolution 58/32. In this regard, Mexico hopes that the report to be submitted to the General Assembly at its sixtieth session will contain substantive recommendations and bring advances in the conceptual and legal definition of the subject.

6. To that end, Mexico is of the opinion that developments and discussions concerning this theme that take place within the framework of other committees of the General Assembly will be helpful, as will relevant provisions contained in international instruments in force and the advances made by other international organizations, such as the United Nations Educational, Scientific and Cultural Organization (UNESCO), in the fields of international security, international terrorism and information, and the information society.

7. As for paragraph 3 of the resolution, concerning "basic notions related to information security", in particular "unauthorized interference with or misuse of information and telecommunications systems and information resources", Mexico emphasizes that the notion of unauthorized interference may give rise to undesirable confusion, inasmuch as it has connotations related to actions undertaken by certain States which, invoking questionable humanitarian and other grounds, interfere, either alone or in concert with others, in the affairs of other States.

8. Thus, the concept might very well be omitted or replaced by "unauthorized access" or simply "illegal access" to refer to acts carried out by certain persons or entities on information systems.

9. In view of the obvious concern with security problems connected with the potential vulnerability of information systems that control the defence programmes of some countries and the risk that computer science and telecommunications may be used by terrorists or for purposes of deterrence, Mexico reaffirms that dialogue, negotiation, international cooperation and international law represent the only ways to make sure that the measures established to deal with problems of information security do not in any way curtail freedom of information or communication.

United States of America

[Original: English]
[13 July 2004]

1. Effective information network and infrastructure security is essential to ensure the reliability, availability and integrity of those national and global information networks on which States and their citizens increasingly depend for essential services and economic security. The issue to be addressed is how nations can act individually and as a community to enhance information network and infrastructure security and prevent debilitating attacks.

2. Some States believe that goal can be accomplished through an international convention that would constrain the development or use of a wide range of information technologies. Implicit in these proposals would be the extension to Governments of the right to approve or ban information transmitted into national territory from outside its borders should it be deemed disruptive politically, socially or culturally.

3. The United States of America does not believe that this approach contributes to the goals of strengthening the security of global information and communications systems, but instead that it contravenes the principle of free flow of information critical to the growth and development of all States. The implementation of information security must not impinge upon the freedom of any individual to seek, receive and impart information and ideas through any media — including electronic — and regardless of frontiers, as set forth in article 19 of the Universal Declaration of Human Rights.

4. By contrast, the United States of America believes that the key threat to cybersecurity originates in the relentless criminal attacks by organized criminals, individual hackers and non-State actors, including terrorists. From this perspective, the benefits of cyberspace can best be protected by focusing both on the effective criminalization by States of the misuse of information technology and on the

systematic national implementation of measures designed to prevent damage to critical information infrastructures no matter the source of the threat — what the United States of America calls the creation of a global culture of cybersecurity. In this view, all parties (government, business, civil society) are aware of their responsibilities and act in ways appropriate to their roles to ensure cybersecurity.

5. With respect to military applications of information technology, an international convention is completely unnecessary. The law of armed conflict and its principles of necessity, proportionality and limitation of collateral damage already govern the use of such technologies.

Cybersecurity through prevention

6. States acting nationally and cooperating internationally to enhance the security of their own critical information infrastructures can best achieve the goal of cybersecurity. Each State should establish a national programme that

(a) Educates and strengthens awareness of best practices in information network and infrastructure security;

(b) Effectively criminalizes misuse of information technology;

(c) Fosters a partnership between government and industry to provide incentives to ensure the security of their national systems;

(d) Establishes a national incident warning and response capability and procedures for sharing information both nationally and internationally.

7. Each State should focus on creating a culture of cybersecurity among all stakeholders, including government, businesses and private citizens, and international cooperation among States towards a global culture of cybersecurity.

8. The report of the Group of Governmental Experts should underscore the approaches contained in General Assembly resolutions 55/63 of 4 December 2000 and 56/121 of 19 December 2001, both entitled "Combating the criminal misuse of information technologies", and 57/239 of 20 December 2002, entitled "Creation of a global culture of cybersecurity". The report could build on these approaches by including language to further the cybersecurity principles that Members have already adopted. Such efforts could be informed by recent multilateral efforts to enhance regional cybersecurity, such as those of the Asia-Pacific Economic Cooperation Telecommunications Forum, the Organization of American States, the World Summit on the Information Society and the Group of Eight.

9. Costly threats to the integrity and availability of national and global information infrastructures originate overwhelmingly from criminal misuse. From the perspective of the United States of America, it is far more important that Governments take steps to ensure that those individuals who engage in such activity can be effectively investigated and prosecuted. For this reason, the United States of America and 34 other States have signed the Council of Europe Convention on Cybercrime of 23 November 2001, which provides guidelines for national legislation and cross-border law enforcement cooperation. The Council of Europe expects to open the Convention to countries not members of the Council, in accordance with its practice and article 37 of the Convention. Indeed, all countries, whether party to the convention or not, can use it immediately as a model for drafting effective domestic laws against cybercrime.

10. Moreover, regardless of the origin of or motivation for an attack, the tools used and the damage suffered by information systems is similar in nature. Thus, it is more important that all nations take systematic steps to reduce the vulnerability of their systems and inculcate in their citizenry a culture of cybersecurity, a set of security practices and habits designed to safeguard their information infrastructures.

11. Effective critical network and information infrastructure protection includes reducing the vulnerability of such infrastructures to all forms of attack so as to minimize damage and recovery time in the event that damage occurs.

12. Effective protection also requires communication, coordination and cooperation nationally and internationally among all stakeholders — industry, academia, the private sector and government entities, including infrastructure protection and law enforcement agencies. Such efforts should be undertaken with due regard for the security of information and applicable law concerning mutual legal assistance and privacy protection. In furthering these goals, States should be encouraged to implement the eleven principles drafted by critical information infrastructure protection experts from the countries of the Group of Eight, and subsequently adopted by the justice and interior ministers of the Group of Eight in May 2003, as they develop a strategy for reducing risks to critical information infrastructures:

(a) Countries should have emergency warning networks regarding cyber vulnerabilities, threats, and incidents;

(b) Countries should raise awareness to facilitate stakeholders' understanding of the nature and extent of their critical information infrastructures, and the role each must play in protecting them;

(c) Countries should examine their infrastructures and identify interdependencies among them, thereby enhancing protection of such infrastructures;

(d) Countries should promote partnership among stakeholders, both public and private, to share and analyse critical infrastructure information in order to prevent, investigate and respond to damage to or attacks on such infrastructures;

(e) Countries should create and maintain crisis communication networks and test them to ensure that they will remain secure and stable in emergency situations;

(f) Countries should ensure that data-availability policies take into account the need to protect critical information infrastructures;

(g) Countries should facilitate tracing attacks on critical information infrastructures and, when appropriate, the disclosure of tracing information to other countries;

(h) Countries should conduct training and exercises to enhance their response capabilities and to test continuity and contingency plans in the event of an information infrastructure attack and should encourage stakeholders to engage in similar activities;

(i) Countries should ensure that they have adequate substantive and procedural laws, such as those outlined in the Council of Europe Convention on Cybercrime and trained personnel to enable them to investigate and prosecute attacks on critical information infrastructures and to coordinate such investigations with other countries as appropriate;

(j) Countries should engage in international cooperation, when appropriate, to secure critical information infrastructures, including by developing and coordinating emergency warning systems, sharing and analysing information regarding vulnerabilities, threats and incidents and coordinating investigations of attacks on such infrastructures in accordance with domestic laws;

(k) Countries should promote national and international research and development and encourage the application of security technologies that are certified according to international standards.

13. Effective network and information infrastructure security can be enhanced by education and training, policy and law, and international cooperation, and may be supported by technology.

14. The United Nations and other multilateral organizations should be supported in their efforts at encouraging member nations to:

(a) Assess the security of their critical national networks and information infrastructures, including understanding their vulnerabilities and interdependencies;

(b) Educate and strengthen national awareness of best practices in information network and infrastructure security;

(c) Effectively criminalize misuse of information technology and facilitate transborder investigations of cybercrime;

(d) Foster a partnership between government and industry to provide incentives to ensure the security of their national systems;

(e) Establish a national incident warning and response capability and procedures for sharing information both nationally and internationally.

Venezuela

[Original: Spanish]
[28 June 2004]

1. The Government of the Bolivarian Republic of Venezuela considers that any violation of information security is contrary to the legitimate right of States to full exercise of their sovereignty. Hence the use of information technologies and media for the purpose of political and economic destabilization is contrary to the fundamental rules of democracy.

2. Information security, then, has a twofold character, inasmuch as it relates both to the guaranteeing of the protection and defence of the information and to its proper use and veracity. Both the illicit use and the deliberate non-use of information and telecommunication systems or information resources for purposes of destabilization constitute disrupting factors in the context of international security.

3. Venezuela supports the elaboration of international principles aimed at enhancing the security of global information and telecommunications systems that make possible or facilitate the fight against terrorism and crime in the sphere of information without prejudicing State sovereignty.